CLAIMS

What is claimed is:

1. A wireless network, comprising:

a plurality of subnetworks, each subnetwork comprising:

at least one network switch; and

at least one air access point comprised of an air interface, an access control module and a router, wherein the router is coupled to the network switch;

at least one router that is connected to the network switch of each of the plurality of subnetworks; and

at least one gateway router that is connected to the plurality of subnetworks.

2. The wireless network as claimed in claim 1, wherein the gateway router is coupled to a mobile telephone network.

3. The wireless network as claimed in claim 1, wherein the gateway router is coupled to a public switched telephone network.

4. The wireless network as claimed in claim 1, wherein the gateway router is coupled to a network operated by a service provider.

5. The wireless network as claimed in claim 4, wherein the service

provider is a virtual operator.

6. The wireless network as claimed in claim 5, wherein a server having a database of mobile subscriber public keys is coupled to the network operated by the service provider.

7. The wireless network as claimed in claim 6, wherein the access control module authenticates a mobile subscriber that is accessing the wireless network by requesting subscriber public keys stored in the database.

8. The wireless network as claimed in claim 1, wherein the at least one gateway router is a plurality of gateway routers.

9. The wireless network as claimed in claim 1, wherein the access module of each of the air access points authenticates a mobile subscriber attempting to access the wireless network through the air interface coupled to the access module.

10. The wireless network as claimed in claim 9, wherein a mobile subscriber is assigned an IP address dynamically when the mobile subscriber accesses the wireless network.

11. A wireless network operated by a plurality of virtual operators,

comprising:

a plurality of subnetworks, each subnetwork comprising:

at least one network switch; and

at least one air access point comprised of an air interface, an access control module and a router, wherein the router is coupled to the network switch;

at least one router that is connected to the network switch of each of the plurality of subnetworks; and

at least one gateway router that is connected to the plurality of subnetworks,

wherein access to services provided by each of the virtual operators is supported by using multiprotocol label switching to route mobile subscriber data between the at least one gateway router and the plurality of subnetworks.

12. The wireless network as claimed in claim 11, wherein at least one of the subnetworks has at least one multiprotocol label switching path so at least one of the virtual operators can be accessed through the air access point of the subnetwork.

13. The wireless network as claimed in claim 11, wherein each of the subnetworks has at least one multiprotocol label switching path so at least one of the virtual operators can be accessed through the air access point of each of the subnetworks.

14. The wireless network as claimed in claim 11, wherein each of the subnetworks has a plurality of multiprotocol label switching paths so a plurality of virtual operators can be accessed through the air access point of each of the subnetworks.

15. The wireless network as claimed in claim 11, wherein each of the plurality of virtual operators is assigned an identification tag that is embedded in a packet header of data that is traversing the wireless network.

16. The wireless network as claimed in claim 11, wherein tunnels based on multiprotocol label switching are provided between the at least one gateway router and the air access point in at least one of the subnetworks.

17. The wireless network as claimed in claim 16, wherein the headers of data packets traversing the wireless network are assigned multiprotocol label switching information, and the network switches of the subnetworks route the data packets through the tunnels based on the headers of the data packets.

18. A method of authenticating a mobile subscriber accessing a wireless network, wherein the mobile subscriber accesses wireless network through an air access point comprising of an air interface and a computer, and the air access point computer is coupled to an database server storing a public key

associated with the mobile subscriber, the method comprising:

sending a first message from the mobile terminal to the air access computer having a user identification number, computing a first codeword, and forwarding the first codeword to the database computer;

sending a second codeword from the database computer to the air access point computer;

extracting a first random character string from the second codeword, and sending a second message comprising the user identification number and a first random character string to the mobile terminal;

sending a third message from the mobile terminal to the air access computer having a user identification number, the first random character string, a second random character string, and a third codeword;

computing a fourth codeword based on the third message received from the mobile terminal, and sending the fourth codeword to the database computer;

computing a fifth codeword at the database computer and sending the fifth codeword to the air access computer; and

computing a sixth codeword and sending a fourth message from the air access computer to the mobile terminal comprised of the user identification number and the sixth codeword.

19. The method of authenticating a mobile subscriber as claimed in claim 18, wherein the air access computer computes the first codeword by performing an authentication encryption of the user identification number using

a secret key.

20. The method of authenticating a mobile subscriber as claimed in claim 19, wherein the secret key is a key known only to the air access computer and the database computer.

21. The method of authenticating a mobile subscriber as claimed in claim 18, wherein the database computer computes the second codeword using the user identification number, the first random character string, a first secret key and a second secret key.

22. The method of authenticating a mobile subscriber as claimed in claim 21, wherein the first secret key is a key known only to the air access computer and the database computer, and the second secret key is a key known only to the mobile subscriber and the database computer.

23. The method of authenticating a mobile subscriber as claimed in claim 22, wherein the first random character string is encrypted using the second secret key to create a first encrypted message.

24. The method of authenticating a mobile subscriber as claimed in claim 23, wherein the first encrypted message is encrypted using the first secret key to create a second encrypted message.

25. The method of authenticating a mobile subscriber as claimed in claim 24, wherein the user identification number, the first random character string and the second encrypted message are encrypted used the first secret key to create the second codeword.

26. The method of authenticating a mobile subscriber as claimed in claim 18, wherein the first random character string is encrypted with a secret key to create the third codeword.

27. The method of authenticating a mobile subscriber as claimed in claim 26, wherein the secret key is a key known only to the mobile subscriber and the database computer.

28. The method of authenticating a mobile subscriber as claimed in claim 18, wherein the fourth codeword is computed using the user identification number, the first random character string, the second random character string, a first secret key and a second secret key.

29. The method of authenticating a mobile subscriber as claimed in claim 28, wherein the first secret key is a key known only to the air access computer and the database computer, and the second secret key is a key known only to the mobile subscriber and the database computer.

30. The method of authenticating a mobile subscriber as claimed in claim 29, wherein first random character string is encrypted using the second secret key to create a first encrypted message.

31. The method of authenticating a mobile subscriber as claimed in claim 30, wherein the user identification number, the first encrypted message and the second random character string are encrypted using the first secret key to create the fourth codeword.

32. The method of authenticating a mobile subscriber as claimed in claim 18, wherein the fifth codeword is computed using the user identification number, the first random character string, a first secret key, a second secret key, and the public key associated with the mobile subscriber.

33. The method of authenticating a mobile subscriber as claimed in claim 32, wherein the first secret key is a key known only to the air access computer and the database computer, and the second secret key is a key known only to the mobile subscriber and the database computer.

34. The method of authenticating a mobile subscriber as claimed in claim 33, wherein the first random character string is encrypted using the second secret key to create a first encrypted message.

35. The method of authenticating a mobile subscriber as claimed in claim 34, wherein the first encrypted message is encrypted using the first secret key to create a second encrypted message.

36. The method of authenticating a mobile subscriber as claimed in claim 35, wherein the user identification number, the first random character string, the second encrypted message and the mobile subscriber's public key are encrypted using the first secret key to create the fifth codeword.

37. The method of authenticating a mobile subscriber as claimed in claim 18, wherein the sixth codeword is computed using the second random character string, a secret key known only to the mobile subscriber and the database computer and the mobile subscriber's public key.

38. The method of authenticating a mobile subscriber as claimed in claim 37, wherein the secret key is a key known only to the mobile subscriber and the database computer.

39. The method of authenticating a mobile subscriber as claimed in claim 38, wherein the second random character string is encrypted using the secret key to create a first encrypted message.

40. The method of authenticating a mobile subscriber as claimed in claim 39, wherein the first encrypted message is encrypted using the mobile subscriber's public key to create the sixth codeword.

41. The method of authenticating a mobile subscriber as claimed in claim 18, wherein the first random character string is generated by the mobile terminal.

42. The method of authenticating a mobile subscriber as claimed in claim 18, wherein the second random character string is generated by the database computer.

43. A computer software product for authenticating a mobile subscriber accessing a wireless network, wherein the mobile subscriber accesses wireless network through an air access point comprising of an air interface and a computer, and the air access point computer is coupled to an database server storing a public key associated with the mobile subscriber, wherein the computer software product comprises:

software instructions that enable the air access computer and the database computer to perform predetermined operations, and a computer readable medium bearing the software instructions, wherein the predetermined operations comprise:

sending a first message from the mobile terminal to the air access

computer having a user identification number, computing a first codeword, and forwarding the first codeword to the database computer;

sending a second codeword from the database computer to the air access point computer;

extracting a first random character string from the second codeword, and sending a second message comprising the user identification number and a first random character string to the mobile terminal;

sending a third message from the mobile terminal to the air access computer having a user identification number, the first random character string, a second random character string, and a third codeword;

computing a fourth codeword based on the third message received from the mobile terminal, and sending the fourth codeword to the database computer;

computing a fifth codeword at the database computer and sending the fifth codeword to the air access computer; and

computing a sixth codeword and sending a fourth message from the air access computer to the mobile terminal comprised of the user identification number and the sixth codeword.

44. The computer software product as claimed in claim 43, wherein the predetermined operations cause the air access computer to compute the first codeword by performing an authentication encryption of the user identification number using a secret key.

45. The computer software product as claimed in claim 44, wherein the secret key is a key known only to the air access computer and the database computer.

46. The computer software product as claimed in claim 43, wherein the predetermined operations cause the database computer to compute the second codeword using the user identification number, the first random character string, a first secret key and a second secret key.

47. The computer software product as claimed in claim 46, wherein the first secret key is a key known only to the air access computer and the database computer, and the second secret key is a key known only to the mobile subscriber and the database computer.

48. The computer software product as claimed in claim 47, wherein the predetermined operations further comprise encrypting the first random character string using the second secret key to create a first encrypted message.

49. The computer software product as claimed in claim 48, wherein the predetermined operations further comprise encrypting the first encrypted message using the first secret key to create a second encrypted message.

50. The computer software product as claimed in claim 49, wherein the predetermined operations further comprise encrypting the user identification number, the first random character string and the second encrypted message using the first secret key to create the second codeword.

51. The computer software product as claimed in claim 43, wherein the predetermined operations further comprise encrypting the first random character string with a secret key to create the third codeword.

52. The computer software product as claimed in claim 51, wherein the secret key is a key known only to the mobile subscriber and the database computer.

53. The computer software product as claimed in claim 43, wherein the predetermined operations further comprise computing the fourth codeword using the user identification number, the first random character string, the second random character string, a first secret key and a second secret key.

54. The computer software product as claimed in claim 53, wherein the first secret key is a key known only to the air access computer and the database computer, and the second secret key is a key known only to the mobile subscriber and the database computer.

55. The computer software product as claimed in claim 54, wherein the predetermined operations further comprise encrypting the first random character string using the second secret key to create a first encrypted message.

56. The computer software product as claimed in claim 55, wherein the predetermined operations further comprise encrypting the user identification number, the first encrypted message and the second random character string using the first secret key to create the fourth codeword.

57. The computer software product as claimed in claim 43, wherein the predetermined operations further comprise computing the fifth codeword using the user identification number, the first random character string, a first secret key, a second secret key, and the public key associated with the mobile subscriber.

58. The computer software product as claimed in claim 57, wherein the first secret key is a key known only to the air access computer and the database computer, and the second secret key is a key known only to the mobile subscriber and the database computer.

59. The computer software product as claimed in claim 58, wherein the predetermined operations further comprise encrypting the first random character string using the second secret key to create a first encrypted message.

60. The computer software product as claimed in claim 59, wherein the predetermined operations further comprise encrypting the first encrypted message using the first secret key to create a second encrypted message.

61. The computer software product as claimed in claim 60, wherein the predetermined operations further comprise encrypting the user identification number, the first random character string, the second encrypted message and the mobile subscriber's public key using the first secret key to create the fifth codeword.

62. The computer software product as claimed in claim 43, wherein the predetermined operations further comprise computing the sixth codeword using the second random character string, a secret key known only to the mobile subscriber and the database computer and the mobile subscriber's public key.

63. The computer software product as claimed in claim 62, wherein the secret key is a key known only to the mobile subscriber and the database computer.

64. The computer software product as claimed in claim 63, wherein the predetermined operations further comprise encrypting the second random character string using the secret key to create a first encrypted message.

65. The computer software product as claimed in claim 64, wherein the predetermined operations further comprise encrypting the first encrypted message using the mobile subscriber's public key to create the sixth codeword.

66. A method of operating a wireless network in which mobile services are provided by a plurality of virtual operators, wherein the wireless network comprises a plurality of subnetworks, each subnetwork comprising at least one network switch, and at least one air access point comprised of an air interface, an access control module and a router, wherein the router is coupled to the network switch, at least one router that is connected to the network switch of each of the plurality of subnetworks, and at least one gateway router that is connected to the plurality of subnetworks, the method comprising:

creating a plurality of multiprotocol label switching paths between the air access point in each subnetwork and the at least one gateway router;

assigning each of the multiprotocol label switching paths to one of the plurality of virtual operators so that the virtual operators can be accessed through the air access point of each of the subnetworks; and

assigning each of the plurality of virtual operators an identification tag that is embedded in a packet header of data that is traversing the wireless network.

67. The method of operating a wireless network as claimed in claim

66, the method further comprising assigning multiprotocol label switching information to the headers of data packets traversing the wireless network, and the network switches of the subnetworks route the data packets through the multiprotocol label switching paths based on the headers of the data packets.

68. The method of operating a wireless network as claimed in claim 66, wherein the method further comprises allowing a mobile subscriber access to a predefined list of services based on the type of subscription that the mobile subscriber has with a virtual operator.

69. The method of operating a wireless network as claimed in claim 66, wherein the method further comprises providing access to a predefined list of services in exchange for advertising.

70. The method of operating a wireless network as claimed in claim 66, wherein the method further comprises excluding access to a predefined set of information sources.

71. The method of operating a wireless network as claimed in claim 66, wherein the method further comprises limiting a mobile subscriber's access to the wireless network based upon a virtual operator's QoS limitations.

72. The method of operating a wireless network as claimed in claim

66, wherein the method further comprises collecting accounting information to be sent to the accounting systems of each virtual operator that provides access to the wireless network.

73. The method of operating a wireless network as claimed in claim 72, wherein the accounting information comprises session duration, requested services and level of service provided.

74. The method of operating a wireless network as claimed in claim 66, wherein the method further comprises assessing each mobile subscriber a flat fee for unlimited access to the wireless network.

75. The method of operating a wireless network as claimed in claim 66, wherein the method further comprises assessing each mobile subscriber a fee for each instance that the mobile subscriber accesses the wireless network.

76. The method of operating a wireless network as claimed in claim 66, wherein the method further comprises assessing each mobile subscriber a fee based upon the total amount of time that a mobile subscriber accesses the wireless network.

77. The method of operating a wireless network as claimed in claim 66, wherein transferring a properly authenticated user from a first air access point

to a second air access point comprises:

fetching the profile of the mobile subscriber from the first air access point and storing it at the second air access point;

signalling the termination of an accounting session that was initiated when the mobile subscriber was granted access at the first air access point;

establishing a new session at the second air access point; and

starting a new accounting session at the second air access point.

78. The method of operating a wireless network as claimed in claim 77, wherein the profile of the mobile subscriber at the first air access point comprises a public key associated with the mobile subscriber, access policies associated with the session at the first air access point, the IP address of the mobile terminal and the session key shared by the mobile subscriber and the first air access point.

79. The method of operating a wireless network as claimed in claim 78, wherein establishing a new session at the second air access point comprises:

generating a session key to be shared by the mobile subscriber and the second air access point;

encrypting both the session key to be shared by the mobile subscriber and the second air access point and the session key shared by the mobile subscriber and the first air access point with the public key associated with the mobile subscriber and forwarding the encrypted result to the mobile terminal;

decrypting the encrypted result and determining if the session key to be shared by the mobile subscriber and the second air access point and the session key shared by the mobile subscriber and the first air access point match; and

if that determination is true, establishing a secure connection between the second air access point and the mobile terminal; otherwise, terminating the access granted to the mobile terminal.

80. The method of operating a wireless network as claimed in claim 79, wherein establishing a new session at the second air access point further comprises informing the at least one gateway router that the mobile subscriber has established a session at the second air access point.